

1 APPEARANCES OF COUNSEL

2 On behalf of the Plaintiffs Donna Curling, Donna
3 Price & Jeffrey Schoenberg

4 DAVID D. CROSS, Esquire
5 Morrison & Foerster LLP
6 2100 L Street, N.W., Suite 900
7 Washington, D.C. 20037-1679
8 202.887.1500
9 dcross@mofo.com

10 On behalf of the Plaintiff Coalition for Good
11 Governance

12 ERIC R. HAVIAN, Esquire
13 Constantine Cannon LLP
14 150 California Street, Suite 1600
15 San Francisco, California 94111-4553
16 415.639.4001
17 ehavian@constantinecannon.com

18 On behalf of the Defendant Brad Raffensperger

19 BRYAN P. TYSON, Esquire
20 Taylor English Duma LLP
21 1600 Parkwood Circle, Suite 200
22 Atlanta, Georgia 30339-2119
23 678.336.7249
24 btyson@taylorenghish.com

25 On behalf of the State Defendants

ALEXANDER DENTON, Esquire
CAREY MILLER, Esquire
JAVIER PICO-PRATS, Esquire
Robbins Alloy Belinfante Littlefield LLC
500 14th Street, N.W.
Atlanta, Georgia 30318
678.701.9381
adenton@robbinsfirm.com
cmiller@robbinsfirm.com
jpicooprats@robbinsfirm.com

1 APPEARANCES OF COUNSEL (continued)

2 DAVID R. LOWMAN, Esquire
Fulton County Attorney's Office
3 141 Pryor Street, S.W., Suite 4038
Atlanta, Georgia 30303-3468
4 404.612.0246
david.lowman@fultoncountyga.gov
5

6

7 ALSO PRESENT:

8 DUNCAN BUELL

9 JENNA CONAWAY, Senior Paralegal, Morrison &
Foerster LLP

10 JILL CONNORS, Legal Assistant, Ichter Davis, LLC

11 MARILYN MARKS, Executive Director
12 SUSAN GREENHALGH, Consultant
Coalition for Good Governance

13 KEVIN SKOGLUND, Citizens for Better Elections

14 Jonathan Miller, Videographer
15

16

17

18

19

20

21

22

23

24

25

1	INDEX		
2	VIRTUAL VIDEOTAPED 30(b)(6) DEPOSITION OF		
3	SANFORD MERRITT BEAVER		
4	Thursday, March 10, 2022		
5	EXAMINATION BY		PAGE
6	By Mr. Cross		268
7	By Mr. Havian		394
8	By Mr. Denton		433
9	DESCRIPTION OF EXHIBITS		
10	EXHIBIT	IDENTIFICATION	PAGE
11			
12	Exhibit 1	Fortalice Solutions Technical	268
13		Assessment Prepared for Secretary	
14		of State Georgia, DRAFT - May 19,	
15		2020, Bates labeled	
16		FORTALICE003593 - FORTALICE003624	
17	Exhibit 2	Fortalice Solutions Firmware	311
18		Comparison and Configuration	
19		Analysis, Secretary of State	
20		Georgia, DRAFT - July 9, 2020,	
21		Bates labeled FORTALICE003807 -	
22		FORTALICE003811	
23			
24			
25			

1	INDEX CONTINUED		
2	DESCRIPTION OF EXHIBITS		
3	EXHIBIT	IDENTIFICATION	PAGE
4	Exhibit 3	Fortalice Solutions Technical	332
5		Assessment Prepared for Secretary	
6		of State Georgia, DRAFT - August	
7		25, 2020, Bates labeled	
8		FORTALICE003692 - FORTALICE003704	
9	Exhibit 4	Fortalice Solutions Technical	345
10		Assessment Prepared for Secretary	
11		of State Georgia, DRAFT - August	
12		25, 2020, Bates labeled	
13		FORTALICE003625 - FORTALICE 003639	
14	Exhibit 5	Fortalice Solutions Technical	352
15		Assessment Prepared for Secretary	
16		of State Georgia, DRAFT - August	
17		25, 2020, Bates labeled	
18		FORTALICE003678 - FORTALICE003691	
19	Exhibit 7	Secretary of State Georgia, Fulton	359
20		County Laptop Forensic Review,	
21		November 25, 2020	
22	Exhibit 8	E-mail string Bates labeled	361
23		FORTALICE001209 - FORTALICE001212	
24			
25			

1	INDEX CONTINUED		
2	DESCRIPTION OF EXHIBITS		
3	EXHIBIT	IDENTIFICATION	PAGE
4	Exhibit 9	E-mail string Bates labeled	369
5		STATE-DEFENDANTS-00104972	
6	Exhibit 10	Security Analysis of Georgia's	373
7		ImageCast X Ballot Marking	
8		Devices, Expert Report Submitted	
9		on Behalf of Plaintiffs Donna	
10		Curling, et al., authored by Prof.	
11		J. Alex Halderman, Ph.D. with the	
12		assistance of Prof. Drew	
13		Springall, Ph.D., dated July 1,	
14		2021	
15	Exhibit 11	Curling Plaintiffs' Fifth Amended	396
16		Notice of Deposition of Office of	
17		the Secretary of State	
18	Exhibit 12	CGG Recording	405
19			
20			
21			
22			
23			
24			
25			

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

INDEX CONTINUED

DESCRIPTION OF EXHIBITS

EXHIBIT	IDENTIFICATION	PAGE
---------	----------------	------

Exhibit 13	Official Election Bulletin, dated November 17, 2020, from Chris Harvey, Elections Division Director, to County Election Officials and County Registrars, RE: Open Records Requests - Security Information Exempt	413
------------	--	-----

(Original exhibits attached to the Original
transcript.)

1 VIRTUAL VIDEOTAPED 30(B)(6) DEPOSITION OF
2 SANFORD MERRITT BEAVER

3 Thursday, March 10, 2022

4 THE VIDEOGRAPHER: We are on the record
5 March 10th, 2022 at approximately 9:09 a.m.
6 Eastern time. This will be Volume II to the
7 30(b)(6) videotaped deposition of the Office of
8 Secretary of State. Representative today will
9 be Sanford Merritt Beaver.

10 Would counsel please identify themselves
11 and who they represent for the record.

12 MR. DENTON: Morning. This is Alexander
13 Denton, here on behalf of the State Defendants.

14 I'll also announce at this time, because I
15 believe his microphone is not connected, that
16 Mr. Pico-Prats, also with our firm, is here on
17 behalf of the State Defendants.

18 MR. CROSS: David Cross of Morrison &
19 Foerster on behalf of Curling Plaintiffs.

20 MR. HAVIAN: Eric Havian, Constantine
21 Cannon on behalf of Coalition for Good
22 Governance.

23 MS. MARKS: This is Marilyn Marks. I'm a
24 Plaintiff's representative for Coalition for
25 Good Governance.

1 MR. TYSON: Good morning. Bryan Tyson for
2 the State Defendants.

3 MR. MILLER: This is Carey Miller, also
4 here for the State Defendants.

5 MR. LOWMAN: This is David Lowman for the
6 Fulton County Defendants.

7 MS. GREENHALGH: Susan Greenhalgh,
8 consultant to Coalition for Good Governance.

9 MS. CONNORS: This is Jill Connors,
10 paralegal for Ichter Davis for Coalition
11 Plaintiffs.

12 THE VIDEOGRAPHER: Thank you.

13 Would the court reporter please swear in
14 the witness.

15 SANFORD MERRITT BEAVER,

16 called as a witness, having been duly sworn
17 by a Notary Public, was examined and testified as
18 follows:

19 EXAMINATION

20 BY MR. CROSS:

21 Q. Good morning, Mr. Beaver.

22 A. Morning.

23 (Plaintiffs' Exhibit 1, [REDACTED])

[REDACTED]

[REDACTED]

1 [REDACTED]
2 marked for identification.)

3 Q. (By Mr. Cross) Would you grab Exhibit 1,
4 please.

5 A. Is it in Exhibit Share?

6 Q. It should be, yes.

7 A. So I'm looking under Curling depositions.
8 I've got deposition of Merritt Beaver, I've got
9 deposition of Merritt Beaver and deposition of
10 Sanford Beaver.

11 Which one of these do you want me to look
12 at?

13 Q. Yes. If you look at the first one,
14 Deposition of Merritt Beaver, Office of Secretary of
15 State. And then you see it's March 10, 2022 is the
16 date. It should be the first one with your name.
17 You will see today's date.

18 A. Okay. Under Marked Exhibits. So
19 Exhibit 1.

20 Got it.

21 Q. Yes.

22 A. Okay.

23 Q. Do you have that in front of you?

24 A. I do.
[REDACTED]

█ [REDACTED] [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

5 A. Yes, I see it.

█ [REDACTED]

█ [REDACTED]

█ [REDACTED] [REDACTED]

█ [REDACTED]

10 Do you see that?

11 A. Yes.

12 Q. And if you flip through it -- if you need a
13 moment to review it, let me know -- but tell me if
14 this is a document you recognize, that you have seen
15 before.

█ [REDACTED]

█ [REDACTED] [REDACTED]

18 Q. So this is a document you saw in the past
19 week?

20 A. Yes.

21 Q. Was that part of your preparation for the
22 deposition today?

23 A. Yes.

24 Q. Just to put this document aside for a
25 moment, what did you do to prepare for today's

1 deposition?

2 A. I went through the different documents that
3 were sent to me. [REDACTED] [REDACTED]

4 [REDACTED]

5 [REDACTED] [REDACTED] [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED] [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 And then there was one other document,
12 which was the red hat report.

13 Q. What's the red hat report?

14 A. A red hat report is basically a report from
15 Fortalice where they take the stance of a malicious
16 attacker to use whatever resources they have to try
17 to breach our system.

18 Q. And do you remember the date, timing of
19 that report?

20 A. I would have to go look at it. I do not.

21 Q. What do you remember about that report?

22 A. Essentially, they talked a lot through
23 their -- the different steps they went through to
24 breach the system from the outside. After going
25 through -- and they documented a number of different

1 approaches they took.

2 At, I think, on the end of -- I think it
3 was Page 6, they defined that they were not able to
4 breach the system with any resources or expertise
5 that they had, and so they moved on to a admitted
6 breach. Admitted breach, meaning we gave them access
7 to a machine as if they were able to breach so they
8 could go into a Phase II to look into moving around
9 our system.

10 Q. When you say "gave them access to a
11 machine," how did you do that?

12 A. We gave them username and password to a
13 computer that was on our network.

14 Q. And why did you give them that access?

15 A. Because they could not get into our system.
16 And the next level of testing was to simulate a
17 breach that had -- potentially had happened, what the
18 potential person could do if they were able to get
19 in. But since they weren't able to breach the
20 system, we make the assumption that "Okay. Let's
21 assume that you are able to get in. Let's give you
22 access as if you were able to breach and then see
23 what you can do." It's a typical exercise when you
24 do red hat.

25 Q. Sorry. You said it's a typical exercise

1 when you do that, and I think I interrupted you.

2 What do you mean by that?

3 A. So red hat is testing basically all your
4 layers of defense in security. If we stop them on
5 the outside so they can't get in, then all we know
6 about our system is that we have got a really good
7 external security layer.

8 But over time things change. People
9 find -- and systems find other vulnerabilities. And
10 if somebody was able to exploit a vulnerability that
11 nobody knew about, then they might be able to get
12 into the system. We still want to know if somebody
13 got into the system what could happen.

14 So we allow somebody a red hat test to get
15 in as if they did breach the system so that they
16 could go to the next level of testing to see, once
17 they got in, what it would look like.

18 Q. And you said this is a typical type of
19 testing. What do you mean it's typical?

20 A. We do an assessment every year. And this
21 is the typical -- there is something called a blue
22 hat, a red hat and a purple hat. Those are security
23 terms for the types of external testing. Red hat is
24 the most aggressive attack.

25 Q. What's a blue hat test?

1 A. That is a -- basically where we give them
2 access to different points ahead of time so they can
3 test, but they know ahead of time how to get in.

4 Q. What's a purple hat test?

5 A. It's a blend of the two.

6 Q. Is the idea with these different types, the
7 red hat and the others, to try to simulate realistic
8 circumstances? You have some sense of
9 vulnerabilities in the real world with your actual
10 system. Is that kind of the idea?

11 A. Yes.

12 Q. The red hat report you said you looked at,
13 is there anything else you remember about it?

14 A. Not off the top of my head, no.

15 Q. Okay. And you said, if I understood you
16 right, so you looked at 20 documents. One was the
17 red hat report. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1 Q. Okay.

2 A. I would have to verify that.

3 Q. So were there any other documents you
4 looked at beyond those 20 to prepare for today?

5 A. No.

6 Q. Was there anyone you spoke with or met with
7 to prepare for today?

8 A. With counsel.

9 Q. Anyone other than counsel?

10 A. Not in specific to prepare for this.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

25 Do you see that?

1

A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

9 Do you see that?

10 A. I do.

[illegible]

██████████ ███████████ ███████████

1	2	3
---	---	---

[illegible]

[illegible]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

7 Do you see that?

8 A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

18 Do you see that?

19 A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

1 [REDACTED]

2 A. Okay. I'm there.

3 Q. (By Mr. Cross) Using the pagination on the
4 page.

5 A. Okay.

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

24 Q. Okay. And it is commonly understood in
25 cybersecurity that the more a particular password is

1 reused across accounts, the greater risk that it is
2 disclosed or it's leaked in some way, right?

3 MR. DENTON: Object to form.

4 You can answer, Merritt.

5 A. Okay. So the answer to that is yes. But
6 that's not what that -- this is talking about here.
7 This is not talking about using the same
8 administrative password for setting up laptops as for
9 accessing servers. This is strictly the password for
10 setting up laptops.

[illegible]

[illegible]

[illegible]

[illegible]

1 [REDACTED]
2 Q. What connections still existed between that
3 Exchange server and other parts of the Secretary's
4 network [REDACTED]

5 MR. DENTON: Objection. Form.

6 A. You need to be clear about what you mean by
7 what connections.

8 Q. (By Mr. Cross) Well, so for example, did
9 individual users still have access to e-mails on the
10 Exchange server at that time?

11 A. No.

12 Q. Did anyone in the Secretary's Office still
13 have access to information on that server?

14 A. IT did.

15 Q. Which I guess what I'm trying to understand
16 is [REDACTED], after the
17 migration from Outlook to 365 but the Exchange server
18 was still set up, it was still accessible by the
19 Internet. And I'm trying to understand, were there
20 any other -- was that server connected in any way to
21 any other parts of the Secretary of State's IT
22 network?

23 A. So at that point in time we had migrated
24 all of our other application servers to a new data
25 center. And so that Exchange server was one of the

1 servers that -- the old equipment that was left in a
2 data center that was no longer being used.

3 But the access to it, from the outside, you
4 could still go in from the outside to it. But there
5 was no connection to the old data center. You would
6 have to go out on the Internet and come back into the
7 new data center through the firewalls.

8 Q. All right.

1 [REDACTED]

2 [REDACTED]

3 [REDACTED]

4 [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[illegible]

[illegible]

■ [REDACTED]

■ [REDACTED]

3 Q. Who had responsibility for determining
4 whether mitigation measures were put in place for
5 each of the vulnerabilities here? Was that you or is
6 that someone else?

7 MR. DENTON: Object to the form.

8 A. Dave Hamilton was in charge at the time for
9 the security group. Jason Matthews was in charge of
10 the infrastructure group. Between the two of them,
11 they sat through the reviews. And we had a regular
12 work schedule of activities that they work on.

13 And they -- basically, if there was
14 something on here that they didn't already know
15 about, then they would add it to their work schedule
16 activities to work on. If it was something they
17 already knew about, then it was just basically "Okay.
18 You identified something we knew about."

19 Q. (By Mr. Cross) As the CIO, did you expect
20 to be informed of any mitigation measures that were
21 taken in response to these vulnerabilities?

22 A. As part of my conversation with those two
23 managers and the regular managers' meetings, I was
24 kept abreast of these -- these conversations were
25 being had that things were being identified and that

1 we were on track to work on them. I did not get into
2 any details of which specific items were identified
3 and what the plan was for working on them.

4 Q. So you relied on Mr. Hamilton and
5 Mr. Matthews to address that; is that fair?

6 A. Correct. This is an annual thing. It's
7 part of our regular working activity along with lots
8 of other things we do to maintain the Secretary of
9 State's network systems. These were focused on our
10 stuff that's exposed to the outside only, things
11 that -- like, voting machines and anything to do with
12 the voting process are not included in these because
13 those weren't attached to any of those systems.

14 Q. So if the voting machines and those types
15 of election systems or election equipment you
16 mentioned aren't part of this annual assessment, is
17 there any separate annual assessment or other
18 assessment Fortalice does on those systems?

19 MR. DENTON: Object to form.

20 A. Those systems are not connected in any way
21 to the outside network Internet. Fortalice helps us
22 understand our exposure to attacks from the Internet.
23 So there wouldn't be -- Fortalice wouldn't be focused
24 on anything like that because those items aren't
25 exposed.

■ ■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ ■ [REDACTED]

5 Q. Why not also rely on their experience and
6 expertise to assess vulnerabilities of equipment
7 that, in the ordinary course, may not be connected to
8 the Internet? Why not have them do that as well?

9 A. We had -- when we first started the
10 election process, they did look at different aspects
11 of that voting system. That was a different
12 contract. That was a different activity. I think
13 you have reviewed that before.

14 Q. And that included the voter registration
15 system, right?

16 A. The voter registration system is part of
17 this.

■ ■ [REDACTED] [REDACTED]

■ [REDACTED], what do you mean
20 by voting systems?

21 A. The balloting system, the actual voting
22 machines and vote counting process.

23 Q. What did Fortalice previously do in cyber
24 assessment of voting machines?

25 A. I would have to go back and review that.

1 As I said, in a prior deposition you covered that,
2 but I would have to go back and rereview that.

3 Q. Are you talking about the DREs or the
4 current BMDs?

5 A. The current BMDs.

6 Q. Was that a specific assessment that was
7 done in late 2019? Is that what you are talking
8 about?

9 A. I would have to go back again. I know we
10 discussed this in a prior deposition and I don't have
11 that current in mind.

12 Q. And -- sorry. I just want to make sure we
13 are talking about the same thing if it's something we
14 talked about before.

15 When you say that Fortalice previously did
16 an assessment of the voting machines, are you talking
17 one specific assessment or are you talking something
18 they did on a regular periodic basis?

19 A. A specific.

20 Q. And you mentioned an assessment of the
21 balloting system. What do you mean by that?

22 A. That would be the Dominion BMD scanners and
23 those systems involved in the voting -- vote
24 collection process.

25

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10 Q. The election results are communicated to
11 the State from the counties through the election
12 night reporting system, right?

13 A. Yes.

14 Q. And those are communicated via the
15 Internet, right?

16 A. Yes.

17 Q. Why not have Fortalice do a security
18 assessment of that system given it's Internet
19 connected?

20 A. That is a cloud service that we buy from a
21 third party vendor. So it's not in our network
22 domain.

23 Q. Who is the cloud service provider for that?

24 A. I think it's Scytl, S-c-y-t-l. May be an
25 "E" on the end.

1 Q. So you rely on the Scytl for the security
2 of that system; is that right?

3 A. Yes.

4 Q. And do you require Scytl to conduct annual
5 cybersecurity assessments of the ENR system?

6 A. We, as part of our contract, give them a
7 security requirements document that they sign off
8 that they have completed and maintain.

9 Q. But that's a document they send back to
10 you, what, each year?

11 A. I don't see a document from them each year.
12 I do get a report from -- I will say from time to
13 time I have seen a report that they have submitted.
14 But I wouldn't say that I get an annual report.

15 Q. How often does that report come in?

16 A. As I said, I don't recall.

17 Q. Do you recall at any point any of those
18 reports identifying any election -- or, I'm sorry,
19 strike that.

20 Do you recall any of those reports at any
21 point identifying any security vulnerabilities or
22 concerns of any kind?

23 A. No.

24 Q. But that's not something you reviewed for
25 today; is that right?

1 A. Correct.

2 Q. Where are those reports maintained at the
3 Secretary's Office?

4 A. I don't maintain any of them.

5 Q. Why is that?

6 A. I don't -- I don't have a reason why.

7 Q. How do you receive them? By e-mail?

8 A. I can't say because I don't know. I can't
9 remember the last one. It's probably been at least a
10 year or two since I remember seeing one.

11 Q. But you don't remember how they get
12 circulated to you?

13 A. The only thing I can say for sure, I can
14 say it's probably e-mail.

15 Q. And so when that comes in -- sorry. Go
16 ahead.

17 A. I said that's how typically communications
18 come in.

19 Q. And so it's your sort of ordinary practice
20 when that comes in, you review it and then you delete
21 the e-mail; is that right?

22 MR. DENTON: Object to form.

23 A. When it comes in, I would more than likely
24 send it to my security, CISA.

25 Q. (By Mr. Cross) So where in the Secretary's

1 Office would you expect those reports to be
2 maintained, if at all?

3 A. I don't have a specific place that I would
4 know to go look.

5 Q. What are the specific security requirements
6 the State has for Scytl?

7 A. There's a document that we give all
8 vendors. It's part of our contracting process.

9 Q. Do you know what the security requirements
10 are in that document?

11 A. I would have to go review it. And over
12 time that document changes as more security things
13 are identified. So back when it was given to them, I
14 don't know -- I couldn't tell you what the document
15 looked like compared to the one that we use now.

16 MR. CROSS: All right. Take a look at
17 Exhibit 2, if you would, please.

18 (Plaintiffs' Exhibit 2, [REDACTED])

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] marked for identification.)

23 Q. (By Mr. Cross) Just let me know when you
24 have it, sir.

25 A. I have got it.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

5 Do you see that?

6 A. Yes.

7 Q. Is this a document you recall seeing
8 before?

9 A. No.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

15 Q. (By Mr. Cross) All right. Take a look at
16 Exhibit 2, if you would, please, and look at the top
17 of Page 2.

18 Again, I'm using the pagination numbers on
19 the document. [REDACTED]

21 Do you see that?

22 A. Yes.

15 A. No.

The diagram consists of 10 horizontal black bars of varying lengths and positions, arranged in a sequence from top to bottom. The bars are as follows:

- Bar 1: Starts at the left edge, ends at approximately 80% width.
- Bar 2: Starts at approximately 15% width, ends at approximately 75% width.
- Bar 3: Starts at approximately 15% width, ends at approximately 60% width.
- Bar 4: Starts at approximately 15% width, ends at approximately 35% width.
- Bar 5: Starts at approximately 15% width, ends at approximately 95% width.
- Bar 6: Starts at the left edge, ends at approximately 98% width.
- Bar 7: Starts at the left edge, ends at 100% width.
- Bar 8: Starts at the left edge, ends at approximately 98% width.
- Bar 9: Starts at approximately 8% width, ends at approximately 32% width.
- Bar 10: Starts at approximately 35% width, ends at approximately 95% width.
- Bar 11: Starts at the left edge, ends at 100% width.

█ [REDACTED]

█ [REDACTED]

3 Do you see that?

4 A. Yes.

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

[illegible]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

17 Does that answer your question?

18 Q. It does, yes. Thank you. It's very

19 helpful.

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

4 A. My understanding is an audit is typically a
5 required activity with a required report. An
6 assessment is an outside opinion.

7 Q. And why has the Secretary's Office done
8 assessments instead of -- and not done audits for
9 cybersecurity purposes?

10 MR. DENTON: Object to form.

11 A. There is no law that requires an audit.
12 There is nothing that requires an audit.

█ █ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[illegible]

[illegible]

11 Q. As a general matter, is it accepted
12 practice, accepted cybersecurity practice to
13 implement updates that are offered to patch
14 vulnerabilities in a system? As opposed to what I
15 think you referred to as, like, a feature
16 enhancement?

17 MR. DENTON: Object to form.

18 A. There are different types of updates.
19 There are different types of updates. Some are more
20 automated, such as blacklisted IP addresses. Those,
21 typically, you automate those. But patches for
22 vulnerabilities, that -- that has to be assessed in
23 your specific environment, whether or not you really
24 want to do that or not.

25 Q. (By Mr. Cross) Under what circumstances

1 would you envision not accepting a patch for a
2 vulnerability in the software?

3 A. Well, patches don't necessarily come in
4 saying "This is for a vulnerability." It just says
5 "patch."

6 Q. So you may not know that a patch coming in
7 includes a vulnerability patch. Is that the idea?

8 A. Not until you research it.

A series of 15 horizontal black bars of varying lengths and positions, representing redacted text lines. The bars are distributed across the page, with some spanning the full width and others being shorter and indented.

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED] █ [REDACTED]

5 Q. All right. Let me grab the next exhibit.

6 And if you want to take a break at any point,

7 Mr. Beaver, just say the word.

8 MR. CROSS: Okay. This is going to be

9 Exhibit 3.

10 All right. You should be able to grab

11 Exhibit 3 now.

12 (Plaintiffs' Exhibit 3, [REDACTED])

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

16 marked for identification.)

17 A. Okay. [REDACTED]

18 Q. (By Mr. Cross) Yes. And so this one is

19 labeled [REDACTED]

█ [REDACTED]

█ [REDACTED]

22 Do you see that?

23 A. Yes.

24 █ [REDACTED]

█ [REDACTED]

[illegible]

21

MR. DENTON: Object to form.

█ [REDACTED]

█ █ [REDACTED]

3 MR. DENTON: Object to form.

█ █ [REDACTED]

█ [REDACTED]

█ [REDACTED]

7 MR. DENTON: Object to form.

█ █ [REDACTED]

█ █ [REDACTED]

█ █ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ █ [REDACTED]

█ █ [REDACTED]

█ [REDACTED] [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ █ [REDACTED]

█ █ [REDACTED]

█ [REDACTED] [REDACTED] [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

[illegible]

[illegible]

[illegible]

[illegible]

1 that these -- the code has these issues.

2 So this is -- what we talked about earlier
3 of you putting layers of security to protect any
4 known vulnerabilities.

5 Q. (By Mr. Cross) And the layer you are
6 talking about now, that would protect against SQL
7 injection, right?

8 A. Yes.

9 Q. And just so we are clear, SQL injection --
10 I guess maybe it's easier to put it this way. SQL
11 injection can occur when a user goes to, like, a
12 website, for example, where they can do a search.
13 And instead of conducting a legitimate search, they
14 put in various terms that causes the system to return
15 information that it shouldn't if it has a
16 vulnerability that allows that. Is that generally
17 right?

18 A. That's -- that's pretty close.

19 Q. Right.

20 A. So our system looks at if you are trying to
21 put in a date field for birth date and you put
22 something else in there, it blocks it. If you have
23 your name, put your name here, and you put in
24 something, a SQL call, it blocks it. And there
25 aren't too many SQL calls that start with Merritt

1 Beaver.

[illegible]

[illegible]

[illegible]

1 Q. And the situation you are talking about is
2 one I think we talked about in the prior deposition
3 that went back -- that came to light shortly before
4 the 2018 election, right?

5 A. Yes. Yes.

[illegible]

█ [REDACTED]

█ [REDACTED]

3 Q. All right. Let me grab the next exhibit.

4 MR. CROSS: This should be Exhibit 4, I

5 believe. Yes.

6 (Plaintiffs' Exhibit 4, [REDACTED])

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

10 marked for identification.)

11 Q. (By Mr. Cross) You should be able to pull
12 that up now, Mr. Beaver.

13 A. Okay. Is this the same one? This is

14 [REDACTED]

█ [REDACTED]

16 Q. Yes, but they are -- hold on. Let me look
17 real quick.

18 [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4 Do you see that?

5 A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] [REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

13

MR. DENTON: Object to form.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

8 Q. All right.

9 MR. CROSS: Let me -- you should be able to
10 pull up Exhibit 5 now, which is -- you'll see
11 it's the third assessment I mentioned before.
12 It's the same date.

13 (Plaintiffs' Exhibit 5, [REDACTED])
[REDACTED]
[REDACTED]
[REDACTED],
17 marked for identification.)

18 Q. (By Mr. Cross) Just let me know when you
19 have that.

20 A. I've got it.

21 Q. And if you come to [REDACTED]

[REDACTED]

[REDACTED]

24 A. Yes.

[REDACTED]

[illegible]

[illegible]

[illegible]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

5 MR. CROSS: All right. Let's take a break.

6 THE VIDEOGRAPHER: Time is 11:09. We are
7 off the record.

8 (WHEREUPON, a recess was taken.)

9 THE VIDEOGRAPHER: The time is 11:16. We
10 are back on the record.

11 MR. CROSS: Grab the next exhibit, if you
12 would.

13 THE WITNESS: Is that 5?

14 MR. CROSS: Exhibit 6.

15 (Plaintiffs' Exhibit 6, [REDACTED])

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED], marked
20 for identification.)

21 MR. DENTON: David, while he's pulling that
22 up, I just wanted to note -- we have had some
23 new people join since we last took roll. It
24 looks like Duncan Buell is now on the call as
25 well. I just wanted to note that for the

1 record. And Phillip Stark, I see.

2 MR. CROSS: Yes. They are both experts.

3 MR. DENTON: I know that. I just -- they
4 weren't here when we started, so I wanted to
5 make sure the record reflected their
6 participation.

7 MR. CROSS: Okay. Thank you.

8 Q. (By Mr. Cross) Do you have Exhibit 6,
9 Mr. Beaver?

10 A. Yes.

[illegible]

18 Q. Oh, I'm sorry. Hold on. I hit the wrong
19 thing.

20 Oh, weird. This happened to Vincent
21 yesterday. There seems to be a glitch with Exhibit
22 Share. Let me try again. For some reason, it looks
23 like it's grabbing the prior exhibit, even though
24 that's not checked.

25 That is weird. I guess Veritext needs to

1 fix this. Hold on. Let me try it again. Let's see
2 if it works this time.

3 A. So it's 7?

4 Q. Yes. So let's go --

5 (Plaintiffs' Exhibit 7, [REDACTED]

[REDACTED]
[REDACTED] marked for identification.)

8 A. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

17 Do you see that?

18 A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

24 Do you see that?

25 A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

16 Q. I'm going to come back to this, but just to
17 help with the context, grab Exhibit 8 if you would,
18 please. And just let me know when you have got it.

19 (Plaintiffs' Exhibit 8, [REDACTED])

[REDACTED]

21 marked for identification.)

22 A. All right. I have it.

23 Q. (By Mr. Cross) And if you come down to the
24 bottom of Exhibit 8, [REDACTED]

[REDACTED]

21 MR. DENTON: Object to the form.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- ■ [REDACTED]
- ■ [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED] [REDACTED]
- [REDACTED]

1. [REDACTED] [REDACTED] [REDACTED] [REDACTED]

2. [REDACTED] [REDACTED] [REDACTED]

3. [REDACTED] [REDACTED]

4. [REDACTED] [REDACTED] [REDACTED]

5. [REDACTED] [REDACTED] [REDACTED]

6. [REDACTED] [REDACTED]

7. [REDACTED] [REDACTED]

8. [REDACTED]

15 Q. All right.

16 Come back to Exhibit 7, if you would. I
17 just had a couple questions on that. [REDACTED]

The diagram consists of 10 horizontal black bars of varying lengths and positions, arranged in a sequence from top to bottom. The bars are as follows:

- Bar 1: Starts at the left edge, ends at approximately 65% width.
- Bar 2: Starts at approximately 15% width, ends at approximately 35% width.
- Bar 3: Starts at approximately 15% width, ends at approximately 85% width.
- Bar 4: Starts at the left edge, ends at the right edge (100% width).
- Bar 5: Starts at the left edge, ends at approximately 80% width.
- Bar 6: Starts at approximately 15% width, ends at approximately 35% width.
- Bar 7: Starts at approximately 15% width, ends at approximately 92% width.
- Bar 8: Starts at approximately 15% width, ends at the right edge (100% width).
- Bar 9: Starts at the left edge, ends at the right edge (100% width).

Row	Bar Length (approx. % of total width)
1	15
2	75
3	100
4	80
5	15
6	85
7	100
8	100

The diagram consists of 20 rows, each represented by a small black square on the left and a horizontal black bar to its right. The bars vary in their vertical position and length relative to the row's bounding box. The sequence of bars is as follows:

- Row 1: A single bar spanning the full width of the row.
- Row 2: A single bar spanning approximately 60% of the row's width, starting from the left.
- Row 3: Two bars. The first starts at approximately 20% width and ends at 30%. The second starts at approximately 20% width and ends at 100%.
- Row 4: Two bars. The first starts at approximately 20% width and ends at 100%. The second starts at approximately 20% width and ends at 95%.
- Row 5: A single bar spanning the full width of the row.
- Row 6: A single bar spanning approximately 85% of the row's width, starting from the left.
- Row 7: A single bar spanning approximately 65% of the row's width, starting from the left.
- Row 8: Two bars. The first starts at approximately 20% width and ends at 65%. The second starts at approximately 45% width and ends at 75%.
- Row 9: A single bar spanning approximately 55% of the row's width, starting from the left.
- Row 10: Two bars. The first starts at approximately 20% width and ends at 75%. The second starts at approximately 20% width and ends at 100%.
- Row 11: Two bars. The first starts at approximately 20% width and ends at 85%. The second starts at approximately 85% width and ends at 100%.
- Row 12: Two bars. The first starts at the left edge and ends at approximately 50% width. The second starts at approximately 55% width and ends at approximately 85% width.
- Row 13: Two bars. The first starts at approximately 20% width and ends at 30%. The second starts at approximately 20% width and ends at 100%.
- Row 14: Two bars. The first starts at approximately 20% width and ends at 100%. The second starts at approximately 20% width and ends at 95%.
- Row 15: A single bar spanning the full width of the row.
- Row 16: A single bar spanning approximately 80% of the row's width, starting from the left.
- Row 17: A single bar spanning approximately 50% of the row's width, starting from the left.
- Row 18: Two bars. The first starts at approximately 20% width and ends at 30%. The second starts at approximately 20% width and ends at 100%.
- Row 19: Two bars. The first starts at approximately 20% width and ends at 100%. The second starts at approximately 20% width and ends at 100%.
- Row 20: A single bar spanning approximately 60% of the row's width, starting from the left.

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11 MR. DENTON: Object to form.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

20 MR. DENTON: Object to form.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

12 MR. CROSS: All right. Grab Exhibit 9,
13 please.

14 (Plaintiffs' Exhibit 9, [REDACTED]
[REDACTED], marked for
16 identification.)

17 Q. (By Mr. Cross) Just let me know when you
18 have that.

19 A. I've got it.

20 Q. And do you see Exhibit 9 is [REDACTED]

[REDACTED]

22 A. Yes.

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

8 Do you recall that?

9 A. I believe so.

10 Q. As of today, have you reviewed that report
11 yourself?

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

22 Q. All right.

23 MR. CROSS: Grab Exhibit 10, if you would.

24 And I'm giving you the redacted version. It has
25 modest redactions, but if you want to see the

1 unredacted, we can do it. But I'm just going to
2 start with the redacted.

3 (Plaintiffs' Exhibit 10, Security Analysis
4 of Georgia's ImageCast X Ballot Marking Devices,
5 Expert Report Submitted on Behalf of Plaintiffs
6 Donna Curling, et al., authored by Prof. J. Alex
7 Halderman, Ph.D. with the assistance of Prof.
8 Drew Springall, Ph.D., dated July 1, 2021,
9 marked for identification.)

10 Q. (By Mr. Cross) So just let me know when you
11 have got it in front of you.

12 A. I got it.

13 Q. As you see, Exhibit 10 says "Security
14 Analysis of Georgia's ImageCast X Ballot Marking
15 Devices," and it's by Professor Halderman, dated
16 July 1, 2021.

17 A. Yes, I see it.

18 Q. And if you need a moment to flip through
19 it, go ahead. But tell me if this is a document you
20 have seen before.

21 A. It looks familiar. I can't recall when I
22 saw it, but it looks familiar.

23 Q. Well, what -- I thought you told me last
24 time that you testified that you had never seen this
25 report and were not even aware of it until recently.

1 A. Well, I think that's -- when I say
2 "familiar," the conversation that's in here looks --
3 sounds familiar. It may have been from our
4 conversation. But prior to that, I have not gone
5 through this in detail.

6 Q. I see. So it could just be --

7 A. Did you not bring this up last time?

8 Q. I did. And that's a fair point. So let me
9 be more specific.

10 A. That's probably when I saw it last.

11 Q. Okay. Okay. That's fair points. Let me
12 be -- let me ask a better question.

13 Have you at any point, as part of your job
14 as a CIO, reviewed this report?

15 A. No.

16 Q. Okay. All right. Thank you. And that's a
17 good clarification.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

8 MR. DENTON: Object to form.

[REDACTED]

10 Q. (By Mr. Cross) Sorry. You said you are not
11 aware?

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

19 MR. DENTON: Object to form.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

25 MR. DENTON: Object to form.

[illegible]

■ [REDACTED]

2 Q. Do you know whether Secretary Raffensperger
3 has reviewed this July 1 report?

4 A. No, I am not aware.

5 Q. If you wanted to know, who would you ask?

6 A. I might ask him.

7 Q. Okay.

8 Okay. Do you know whether Jordan Fuchs has
9 reviewed the July 1 report from Dr. Halderman?

10 A. I'm not aware of anything about this report
11 with anybody at SOS.

12 Q. So as you sit here, you are not aware of
13 anyone at the Secretary's Office -- you can't
14 identify anyone who has read this report; is that
15 fair?

16 A. That's fair.

17 Q. Have you -- well, I guess to give it some
18 context, do you understand that this report has gone
19 to CISA at DHS?

20 A. (Unintelligible.)

21 Q. I'm sorry. There's some static.

22 A. I said other than you just telling me that.

23 Q. Can you hear me?

24 A. Can you hear me?

25 THE VIDEOGRAPHER: I'm getting some really

1 bad static as well, Counsel.

2 MR. CROSS: Okay. Sorry.

3 THE WITNESS: Am I okay now, or am I still
4 staticky?

5 THE VIDEOGRAPHER: It sounds like it's
6 coming from the witness' end.

7 THE WITNESS: Did it just start?

8 MR. CROSS: Yes.

9 THE WITNESS: Can I get a phone or
10 something?

11 THE VIDEOGRAPHER: Would you like to go off
12 the record, Counsel, while we address the issue?

13 MR. CROSS: Yes, let's do that.

14 THE VIDEOGRAPHER: The time is 11:42. We
15 are off the record.

16 (WHEREUPON, there was a discussion off the
17 record.)

18 THE VIDEOGRAPHER: The time is 11:44. We
19 are back on the record.

20 Q. (By Mr. Cross) All right. Mr. Beaver, I'm
21 almost done. I was just asking you have you -- had
22 you heard that CISA now has a copy of this July 1
23 report from Dr. Halderman?

24 A. No.

25 Q. Do you have any view on whether the report

1 should be public? Publicly released?

2 A. I don't think that's my decision.

3 Q. Okay. But you are the Chief Information
4 Officer for the Secretary's Office. [REDACTED]

5 [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 A. Anything that can adversely effect
10 security, in my opinion, shouldn't be released. You
11 are only reducing Georgia's ability to secure their
12 equipment and systems whenever security information
13 about an existing system is released. In my mind,
14 it's bad practice and just, you know, being ignorant
15 of cybersecurity.

16 Q. Last couple questions or couple points.

17 What are the industry-recognized benchmarks
18 that the Secretary's Office attempts to adhere to for
19 cybersecurity for the voting system, if any?

20 MR. DENTON: Object to form.

21 A. That is way too broad of a question.

22 MR. CROSS: Fair enough. Let me narrow it
23 down. Let's just focus on the Dominion
24 equipment, the BMDs, the printers, the scanners.

25 Q. (By Mr. Cross) What, if any,

1 industry-recognized benchmarks does the Secretary's
2 Office try to adhere to for securing that equipment?

3 A. Once again, you are -- it's a very broad
4 question. You would have to be very specific.
5 Everything from physical to software to wireless and
6 hard networks, there's a whole range of attack
7 vectors to take into consideration. We use that
8 word. It's a common term in cybersecurity.

9 So when you say what avenues, I mean,
10 someone could talk for days on the attack vectors
11 that one should look at. So I can't be specific with
12 it, that broad of a question.

13 Q. And why should one look at the attack
14 vectors of that equipment?

15 A. Basically attack vectors are where systems
16 can be compromised. And so reducing attack vectors
17 is always your first defense. And then once you have
18 vectors that you can't get rid of, then what do you
19 do on those vectors?

20 Q. If I wanted to understand -- or strike
21 that.

22 If I wanted to understand what the
23 industry-recognized benchmarks are that the
24 Secretary's Office attempts to adhere to with the
25 voting equipment that we -- just the Dominion

1 machines, is there someplace I can look? Like, are
2 there industry treatises? Is there some source that
3 I could turn to to get a sense of what those
4 standards are?

5 MR. DENTON: Object to form.

6 A. I don't have one I can point you to.

7 Q. (By Mr. Cross) Are you familiar with the
8 concept of software independence?

9 A. That's a concept. I have not heard it as a
10 term.

11 Q. Sorry. Make sure I understand your answer.
12 You are or are not familiar with software
13 independence?

14 A. I have an idea what it might be, but could
15 be multiple things. So if you are saying that is an
16 industry term that means something specific, I don't
17 know what you are talking about.

18 Q. And when you say you have an idea of what
19 it might be, what's the idea that you have in mind?

20 A. Software independence could be a software
21 that a company has that is proprietary that nobody
22 else can use. Software independence could be
23 something that could stand on its own in an
24 environment to do some activity.

25 There's lots of ways you might use those

1 terms when speaking to software. But if it's an
2 industry term that that means, I don't know what it
3 is.

4 Q. Okay. And when you say it could mean
5 software could stand on its own in an environment,
6 what do you mean by that?

7 A. Such as a cash register, by itself, doesn't
8 have to plug into anything else. It can stand on its
9 own and do what it needs to do.

10 Q. Without interacting with some other
11 software or system?

12 A. Exactly.

13 Q. Okay.

14 A. That would be a term that, if you said
15 that's what it means, I would understand what you are
16 saying.

17 Q. In that situation -- just so I understand
18 what you are saying -- the cash register would depend
19 on the software for its operation, but it wouldn't
20 depend on other software for its operation. Is
21 that --

22 A. Other software or outside connections,
23 let's say.

24 Q. Okay.

25 A. But I don't know if that's truly what that

1 means. That was just an example of what that one
2 interpretation might be.

3 Q. Understood.

4 Last topic and then I'm done.

5 Are you an employee of the Secretary's
6 Office?

7 A. I'm a contractor.

8 Q. Contractor. And do you -- is your --
9 strike that.

10 Do you have a contract with the Secretary's
11 Office that governs your role as CIO?

12 A. Every year I sign a contract.

13 Q. So you renew a contract each year?

14 A. Correct.

15 Q. And I'm sorry, just remind me, how many
16 years have you been the CIO?

17 A. Since 2014.

18 Q. And have you always been a contractor?

19 A. It has varied -- it has varied over the
20 years.

21 Q. What years were you an employee of the
22 Secretary's Office?

23 A. I think '15 I was an employee.

24 Q. Any other years you think you --

25 A. Well, actually, I was not an employee. I

1 was a temp. I started off as a contractor and I went
2 to be a temp and then I went back to a contractor.

3 Q. So there has not been a period where you
4 were an employee of the Secretary's Office, you were
5 either a contractor or a temp?

6 A. Yes.

7 Q. And what's the difference between a
8 contractor and a temp?

9 A. I think it's an administrative or
10 accounting term and how they can pay people.

11 Q. What's the difference in your experience?

12 A. One, I get a check from the Secretary of
13 State. And one, I get a check from a third party
14 vendor.

15 Q. I see. So when you were a temp, you were
16 working through a third party vendor and your
17 compensation came through that vendor?

18 A. Opposite.

19 Q. Oh. Oh, I'm sorry. So when you were a
20 temp, you were paid directly by the Secretary's
21 Office, but not as an employee. When you were a
22 contractor, your comp comes through a third party
23 vendor?

24 A. When I was a temp, I got paid by the
25 Secretary of State as a temp. When I initially

1 started, I was paid by a third party. Then I became
2 my own contractor.

3 Q. And you became your own contractor after
4 you were a temp?

5 A. Correct.

6 Q. And when you were a contractor before you
7 were a temp, who was the third party that you were
8 working through?

9 A. That was a long time ago. I don't recall.
10 It seems to me it started with a "K." They were out
11 of Minnesota.

12 Q. How did you get the job as CIO?

13 A. I was recruited by a contracting firm.

14 Q. Was that the same contracting firm that you
15 were compensated through?

16 A. Yes.

17 Q. That firm recruited you -- was it
18 specifically for the CIO role at the Secretary's
19 Office?

20 A. Yes. Yes.

21 Q. And do you have any insight into why the
22 Secretary has never brought you in as an employee of
23 the office?

24 A. I can only speculate.

25 Q. Okay. That's fine. I don't want you to

1 guess.

2 Have you ever had any discussions or
3 communications with anyone in the Secretary's Office
4 about why you are not an employee?

5 A. No. I mean, I have talked to them about
6 being a contractor. Basically it's "How do you want
7 to, this relationship, work?"

8 Q. And so is it your --

9 A. So I have not approached them and said
10 "Hey, I want to be an employee."

11 Q. Is it your preference to be a contractor?

12 A. Yes.

13 Q. And why is that?

14 A. I have more control of what I do.

15 Q. In what sense?

16 A. Right now I'm a CIO for multiple agencies.

17 Q. Got it. So if you were an employee of the
18 Secretary's --

19 A. I couldn't do that as an employee.

20 Q. And I don't think I asked you this before.
21 I'm sorry if I did.

22 What is your annual compensation as a
23 contractor for the CIO role?

24 A. 120,000.

25 Q. And that's current?

1 A. That's current.

2 Q. And has that gone up in the time that you
3 have been in that role?

4 A. It changes from time to time, up and down.

5 Q. What's the highest it's been in a given
6 year to the best of your memory?

7 A. It was around 200 at one time.

8 Q. Do you recall when that was?

9 A. I think in '18.

10 Q. And what was the lowest?

11 A. Probably when I got started, it was around
12 a hundred.

13 Q. And what factors go into determining
14 compensation for any given year?

15 MR. DENTON: Object to form.

16 A. I don't -- you would have to ask Secretary
17 of State what they value in a CIO.

18 Q. (By Mr. Cross) Do you negotiate your comp
19 for your contract or they just tell you "This is what
20 we are going to pay you"?

21 A. It's a negotiation, like anything.

22 Q. Okay.

23 A. It's a contractor. I'm a contractor. I
24 negotiate all services.

25 Q. And I guess what I'm trying to understand

1 is when you negotiated your compensation with the
2 Secretary's Office, what was your understanding of
3 the factors that went into deciding what that
4 ultimate number would be?

5 A. Performance. I was the fifth CIO in two
6 years when I started. Secretary of State's Office
7 was struggling to find the right person that could
8 handle what -- their environment.

9 Q. And why was that a struggle?

10 A. Managing the different agencies is a
11 challenge. Understanding the difference between
12 vendor management, internal systems management and
13 security and politics is not something typically they
14 found in the people they hired.

15 Q. To your understanding, why is your
16 compensation as CIO, why did it go from a high of
17 200,000 in or about 2018 to 120 now?

18 A. Because I picked up another agency.

19 Q. And are you doing less work for the
20 Secretary now than you were before?

21 A. You say "less work." I'm still managing
22 the same responsibility. I have just built a team --
23 I have just built a team that can carry the load
24 better.

25 Q. Yes. That was a bad question. Let me ask

1 it different.

2 When I say "less work," are you working
3 fewer hours in your role as CIO now than you were in,
4 say, 2018 when you had a higher pay level?

5 A. Today I work in two different
6 organizations. So I spend -- there's only 24 hours
7 in a day. So I -- of course I have to spend time in
8 my other agency. So, I mean, that's -- I'm
9 considered a fractional CIO now.

10 Q. And how long have you been a fractional
11 CIO?

12 A. Well, I have been -- I think about two
13 years.

14 Q. And how --

15 A. It was after Kemp left.

16 Q. About how much of your working hours would
17 you say you spend -- whatever metrics is easier for
18 you, weekly, monthly -- working for the Secretary as
19 a CIO?

20 A. It completely varies. Right now, I'm
21 spending an awful lot of time. Other times, I spend
22 more time in my other agency. So I don't have a set
23 calendar of time.

24 Q. Were you to do it over the course of a
25 year, how would say it breaks out roughly?

1 A. I have never tried to assess that.

2 Q. What would your best assessments? Is
3 it 50/50? If it swings, is it closer to more -- one
4 agency over the other?

5 MR. DENTON: Object to form.

6 A. I don't know. I would be speculating and I
7 don't want to speculate.

8 Q. (By Mr. Cross) Do you keep track of your
9 hours?

10 A. No.

11 Q. So you're compensated on a salary basis?

12 A. Correct. Doing the job, not hours.

13 Q. And you said your other agency, what's the
14 other agency?

15 A. Office of the Commissioner of Insurance.

16 Q. And have you had that role since 2019 or
17 2020?

18 A. 2020.

19 Q. Are there any other jobs that you have
20 beyond the insurance agency and Secretary's Office?

21 A. Not at this time.

22 Q. Are there any other jobs that you have had
23 while you were the CIO of the Secretary's Office?

24 A. No.

25 Q. Let me just look at my notes real quick.

1 Do you have any other contractors or temps,
2 anyone who works for you, who is not an employee of
3 the Secretary's Office?

4 A. I have nobody working for me under my
5 contract. I have people who work for me at the
6 Secretary of State.

7 Q. Are those individuals all employees at the
8 Secretary's Office?

9 A. Some are contractors. But not working for
10 me.

11 Q. Who are the contractors?

12 A. I think IDR is one. Inside Global is
13 another. We may have a couple of independents.

14 Q. Do you have any insight into how the
15 decision gets made at the Secretary's Office to bring
16 somebody in, particularly at a senior level, on a
17 contract basis rather than an employee basis?

18 A. In IT, since I have started there, we have
19 typically done contract to hire almost, I would say,
20 90 -- 90 percent of the time. It is a good practice
21 in the IT arena that I have used for years is do
22 contract to hire.

23 Q. Why is that?

24 A. The IT -- the IT world is -- sorry.
25 Somebody is at the doorbell.

1 IT world is -- is a hot market. And so
2 being able to assess people in just an interview with
3 what they say versus what they can actually do is
4 difficult. So I find it's better to contract with
5 them for three to six months, see if they really can
6 do what they say. And then after that, if I want to
7 bring them on board, I will bring them on board.

8 Q. Who are the names of the individuals at
9 Secretary's Office that you are familiar with who
10 work with the IT Department who are on a contract
11 basis? You mentioned some roles or some positions.
12 Who are the individual names?

13 A. You mean, like, in my -- people in my
14 department?

15 Q. Yes. Any -- you mentioned particular roles
16 that you understand are on a contract basis. Who
17 fills those roles? What are the names of the people?

18 A. I mean, who fills them?

19 Q. Yes.

20 A. Well, all contracting has to come through a
21 company called CAI.

22 Q. No, I'm sorry. I'm saying who are the
23 names of those individual people in those roles
24 currently?

25 A. So you are asking for the name of the

1 people that are on my staff?

2 Q. Yes, who are on a contract basis, rather
3 than an employee?

4 A. I would have to get my org chart out. So,
5 I mean, I have got 22 people and probably 50 percent
6 of them are contractors. So I have -- I would have
7 to get an org chart.

8 Let me shut the door.

9 Q. All right. I'm almost done, Mr. Beaver.

10 So about half of your team is on a contract
11 basis. Do the roles and responsibilities change for
12 people on your team on whether they are an employee
13 of the Secretary's Office versus a contractor?

14 A. No.

15 Q. Does the compensation vary in any way?

16 A. Well, not everybody makes the same thing.
17 So depending on -- compensation goes by role, not by
18 contract versus a full-time equivalent. FTEs, we
19 call them. So -- but an FTE could be filled by a
20 contractor -- or a position could be filled by a
21 contractor or an FTE. Typically, the pay is similar.

22 Q. Are there any documents you brought with
23 you today other than the Fortalice reports that you
24 looked at?

25 A. No. I think I have learned from the past.

1 Q. All right.

2 MR. CROSS: I don't have any further
3 questions for you, Mr. Beaver. I understand
4 another lawyer for some other Plaintiffs will
5 ask you some questions.

6 But thank you. I appreciate you taking the
7 time.

8 THE WITNESS: Okay. Can we take two
9 minutes so I can see who's at the front door?

10 MR. HAVIAN: Yes. Actually, let's take ten
11 minutes because I want to pull stuff together
12 and then we will go back on the record and I
13 will be finishing up with you. Okay?

14 THE WITNESS: Thank you.

15 THE VIDEOGRAPHER: The time is 12:04. We
16 are off the record.

17 (WHEREUPON, a recess was taken.).

18 THE VIDEOGRAPHER: The time is 12:14. We
19 are back on the record.

20 EXAMINATION

21 BY MR. HAVIAN:

22 Q. Good afternoon, or I guess it's just
23 afternoon your time, Mr. Beaver. This is -- my name
24 is Eric Havian and I am appearing for the Coalition
25 for Good Governance. We have a total of an hour and

1 14 minutes that we are allotted to question you, but
2 I know it's lunchtime back there. So I'm going to
3 ask do you guys -- are you okay just going through
4 and finishing or would you prefer to take a break and
5 get something to eat?

6 A. I prefer just finishing.

7 Q. Okay. That's what most witnesses prefer to
8 do, but I figured I would give you the choice.

9 MR. DENTON: Eric, before you continue, I
10 just have -- have you made an appearance in this
11 case?

12 MR. HAVIAN: Yes, I have a pro hac vice
13 application that's currently pending.

14 MR. DENTON: Okay. So you haven't made an
15 appearance?

16 MR. HAVIAN: We checked the rules. It's
17 our understanding of the rules in Georgia that I
18 don't need to make a formal appearance. If I
19 have made a pro hac vice application, that
20 serves as my Notice of Appearance.

21 MR. DENTON: That's fine. I just wanted to
22 understand.

23 MR. HAVIAN: Yes. I presume you should be
24 served at some point electronically with the pro
25 hac application I filed.

1 MR. DENTON: Yes, I saw the application. I
2 just haven't seen anything further.

3 Thank you.

4 MR. HAVIAN: You are welcome.

5 (Plaintiffs' Exhibit 11, Curling
6 Plaintiffs' Fifth Amended Notice of Deposition
7 of Office of the Secretary of State, marked for
8 identification.)

9 Q. (By Mr. Havian) Okay. Mr. Beaver, let's
10 jump right in. I would like to have you take a look
11 at Exhibit 11.

12 A. Okay.

13 Q. Which is a Notice of Deposition. And the
14 pages, at least on my copy, do not appear to be
15 numbered. But if you could -- if you could scroll
16 down to Topic Number 10, which is about
17 three-quarters of the end of the document.

18 A. Does it start with any instance in 2020 and
19 2021?

20 Q. Correct. That says "Any instance in 2020
21 or 2021, within the knowledge of the Secretary of
22 State's Office, when a person or entity other than an
23 authorized election worker or Georgia state or county
24 official obtained voting data from a Georgia election
25 or images of voting equipment used in a Georgia

1 election."

2 Do you see that?

3 A. Yes.

4 Q. That's going to be the primary area of my
5 focus today. Are you prepared to address that issue
6 today?

7 A. I can answer to my knowledge.

8 Q. Have you taken any steps to gather
9 knowledge of any other persons in the Georgia
10 Secretary of State's Office about this issue?

11 A. No.

12 Q. Okay. I believe it was yesterday or
13 perhaps the evening before yesterday, Mr. Bruce
14 Brown, counsel for the Coalition, sent an e-mail to
15 Mr. Russo and Mr. Miller asking that you, in
16 particular, focus on a particular aspect of Issue
17 Number 10. And I'll read that to you. It says "That
18 examination will focus primarily on the events
19 discussed in the audio recording marked as Exhibit 12
20 and played at the deposition of Gabriel Sterling
21 involving the imaging of election hardware and
22 software in Coffee County. Please ensure that the
23 witness is prepared to address that aspect as well as
24 the other aspects of Issue 10."

25 I guess my question is, are you aware --

1 and I don't want to get into discussions with
2 counsel -- but are you aware that it was our
3 intention to focus especially on the incident in
4 Coffee County?

5 A. I was told that that question came up.

6 Q. Okay. Are you prepared to address that
7 issue?

8 A. I can tell you my knowledge of it.

9 Q. Have you taken any steps to go beyond your
10 personal knowledge with regard to that topic?

11 A. No. I just heard about it.

12 Q. I understand.

13 A. We don't -- we have less than -- less than
14 a day notice on this.

15 Q. On that particular aspect, yes, I
16 understand. Although you've had considerably longer
17 notice about Issue Number 10, correct?

18 A. Issue Number 10, you mean knowledge of any
19 person other than authorized election workers,
20 counties obtained voting data from Georgia?

21 Q. Correct.

22 A. And I have no knowledge of anybody that
23 aren't authorized getting any voter data.

24 Q. Okay. So -- and as I understand your
25 testimony, you have not taken any steps to

1 investigate whether anyone else at the Georgia
2 Secretary of State's Office has any knowledge of
3 unauthorized election workers allowing voting data to
4 be copied?

5 A. Yes, no one has --

6 MR. DENTON: Objection to form.

7 A. No one has reported to me anything that
8 would state that there was any non-authorized people
9 getting data.

10 Q. (By Mr. Havian) What steps did you take to
11 investigate whether anyone had such information?

12 A. As I said, I just learned about this
13 question. So none.

14 Q. Okay. So let me -- I apologize because
15 there are two separate issues I'm talking about.
16 There's a narrower question of Coffee County. I want
17 to focus on the broader question.

18 What steps did you take to investigate
19 whether any person or entity other than authorized
20 election workers obtained voting data from a Georgia
21 election or images of voting equipment used in a
22 Georgia election?

23 A. And as I said, I have --

24 MR. DENTON: Object to form.

25 A. -- only heard about Question 10 for less

1 than a day.

2 Q. (By Mr. Havian) So until yesterday, you
3 were not aware of Topic Number 10 at all; is that
4 correct?

5 MR. DENTON: Object to form.

6 Q. (By Mr. Havian) Just so I clarify, by
7 Topic 10, I'm referring to Topic Number 10 that's
8 stated in Exhibit 11 that you are looking at now.

9 A. Correct.

10 Q. Okay. So after you learned about Topic
11 Number 10 yesterday, you didn't have -- is it fair to
12 say you just didn't have sufficient time to speak
13 with others in the Georgia Secretary of State's
14 Office to see if anyone else might have information
15 on that topic? Is that fair?

16 A. That would be fair.

17 Q. If you did have more time to inquire, who
18 would you speak to about Topic Number 10 to find out
19 what the Georgia Secretary of State's Office knew
20 about it?

21 A. I would speak to probably the head of the
22 elections group, Blake Evans. Probably would speak
23 to my security person, although if he had heard of
24 anything -- I say person, my security manager -- if
25 he had heard something, he would have probably told

1 me.

2 So the fact that I didn't hear anything
3 from him, I know his answer. I might talk to Gabe
4 Sterling. I might talk to Michael Barnes. Those
5 would be my starting points.

6 Q. And who is the security person that you are
7 referring to?

8 A. Kevin Fisk.

9 Q. All right. So let me ask you a few other
10 questions, more general questions about Coffee
11 County.

12 First of all, are you aware that
13 Mr. Gabriel Sterling gave a deposition in this matter
14 as well?

15 A. I just heard about it. I have no details
16 on it.

17 Q. I'm going to read to you something that
18 Mr. Sterling said in his deposition and ask you
19 whether you agree with his statement or not.

20 Mr. Sterling testified, quote, "Physical
21 security is the -- obviously, the frontline of all
22 cybersecurity. And that's one of our main things we
23 have to worry about at all times. That's why we --
24 we work with the counties to make sure they have
25 these things in under lock and key," close quote.

1 Do you understand the sentence I just read
2 to you about physical security?

3 A. Yes, I do.

4 Q. Do you agree with Mr. Sterling's testimony?

5 A. I do.

6 Q. Can you explain why physical security is so
7 important in election security?

8 A. Physical security is one vector of attack
9 for someone who is trying to do some malicious damage
10 to the environment. So protecting physical access is
11 one avenue that you have to go after to make sure
12 that the system is secure.

13 Q. To your knowledge, has the Secretary of
14 State taken any steps since the 2020 Presidential
15 election to investigate the physical security of the
16 election hardware and software in Coffee County?

17 A. In Coffee County? I -- specifically, that
18 county, I can't speak to. I know that we do a number
19 of things to monitor all counties, so Coffee would be
20 included in that.

21 So -- but I don't know of anything
22 specifically targeting Coffee County. Coffee would
23 be included in the -- in the monitoring for physical
24 security that is done across all counties.

25 Q. Okay. Do you know -- can you describe for

1 us the activities taken across all counties to
2 investigate the physical security of the hardware and
3 software in the election system?

4 MR. DENTON: Object to form.

5 A. Yes. I don't have the specific
6 requirements for each county. Each of them are
7 required to store all the equipment in a secure
8 location that is locked and monitored. Monitor is
9 either -- you know, includes video and surveillance,
10 like, Security checking on it on a regular basis.

11 But I don't have any specific document that
12 I can point to that says here's what all the counties
13 do. That -- you would have to talk to somebody in
14 the Elections Department and -- to see what are some
15 of the common things that are identified for counties
16 to do. That's not my role.

17 Q. (By Mr. Havian) Would the copying or
18 imaging of data, election data or election software
19 or hardware, would that be a violation of the
20 physical security requirements if done by anyone
21 other than an authorized election worker?

22 MR. DENTON: Object to form.

23 You can answer if you understood the
24 question, Merritt.

25 A. I think the question is obvious that yes,

1 that would be a breach of security, although I have
2 yet to hear of any breach, although we do get many
3 people who claim to do breaches that have never been
4 proved. I would suspect that if there is such a
5 claim right now, until someone can actually prove
6 that that was done, that it would be in question as
7 to the actual reality of that actually happening.

8 Q. (By Mr. Havian) So --

9 A. Has anybody tested that?

10 Q. Well, I'm not allowed to answer questions
11 you ask me, although sometimes I would really enjoy
12 doing that, but that violates the rule. So I'm
13 afraid I'll have to leave you in suspense on that
14 question.

15 I take it from your answer, is it fair to
16 say that imaging election software or other election
17 data is a serious, serious breach of security --

18 MR. DENTON: Object to form.

19 Q. (By Mr. Havian) -- if it happened?

20 A. It is a breach of security.

21 Q. Do you consider it a very serious breach of
22 security if it, in fact, occurred?

23 A. Breach of security is serious. It's not
24 something I would ever want to happen.

25 Q. Okay. And I take it from your testimony

1 that you have never seen an example in Georgia of
2 anyone breaching security in this manner; is that
3 fair?

4 MR. DENTON: Object to form.

5 A. That's more than fair. That is accurate.

6 Q. (By Mr. Havian) Okay. Have you ever heard
7 about such breaches occurring in other jurisdictions?

8 A. You mean other jurisdictions, you mean
9 other states?

10 Q. Yes.

11 A. No, I have not heard other states that had
12 that problem either. It doesn't mean it happened. I
13 just haven't heard it.

14 (Plaintiffs' Exhibit 12, CGG Recording,
15 marked for identification.)

16 Q. (By Mr. Havian) I would like to play a
17 recording for you. It's been uploaded as an exhibit.
18 And that will be --

19 A. Do you want me to download it?

20 Q. Well, it should show up. Hopefully, it's
21 going to show up on your screen in the same way as
22 any other exhibit. And if you click on it it should
23 play.

24 A. Exhibit 12?

25 Q. Exhibit 12, correct.

1 A. Do you want me to play it or are you going
2 to play it?

3 Q. I think you have to play it, I believe.

4 A. All right.

5 It's two minutes and 35 seconds. Do you
6 want me to listen to the whole thing?

7 Q. Please.

8 (WHEREUPON, the recording was played.)

9 Q. (By Mr. Havian) Were you able to hear that
10 okay, Mr. Beaver?

11 A. Yes. Yes.

12 Q. Have you ever heard that recording before?

13 A. No.

14 Q. I will represent to you that the female
15 voice on that recording is Marilyn Marks, who is
16 associated with the Coalition for Good Governance.

17 Do you recognize the male voice?

18 A. No.

19 Q. You have never heard it before?

20 A. No.

21 MR. DENTON: Object to the form.

22 Q. (By Mr. Havian) Does the name Scott Hall,
23 does that mean anything to you?

24 A. No.

25 Q. You have never heard that name before?

1 A. Never heard that name before.

2 MR. DENTON: Object to form.

3 Q. (By Mr. Havian) The events described on
4 this audio recording, if those events really
5 occurred, would they constitute a violation of
6 Georgia election rules as you understand them?

7 MR. DENTON: Object to form.

8 A. Yes. But his comments kind of lead me to
9 believe that he's not very technical and really
10 doesn't know what he's talking about. So I would be
11 highly suspect of anything he's saying.

12 Q. (By Mr. Havian) Did you understand him to
13 be saying that he did something technical himself as
14 opposed to observing others doing technical things?

15 A. He was observing others doing technical
16 things and was not able to very accurately reflect
17 what potentially could have happened.

18 Q. Can you explain further what you mean by
19 that?

20 A. Poll pads don't have a hard drive. Yet he
21 said they imaged the hard drive on a poll pad. I
22 would guess he doesn't know what he's talking about.

23 Q. Can --

24 A. So that kind of puts the whole conversation
25 in question as to really did he know what he was

1 seeing going on.

2 So I would definitely would want somebody
3 who actually understood technology and understood
4 what was potentially going on there to do before I
5 jumped to any conclusions. Sounded like somebody was
6 trying to brag and get somebody's attention.

7 Q. So I -- you're at somewhat of a
8 disadvantage because I have an informal writeup of
9 what he said on the audiotape. And I apologize we
10 didn't have a transcript for you. But I don't recall
11 him saying that the poll pad was imaged.

12 A. He said he imaged everything.

13 MR. DENTON: Merritt, let Mr. Havian finish
14 his question before you start to answer.

15 Q. (By Mr. Havian) My question is, did you
16 hear him specifically say that he imaged the poll
17 pad?

18 MR. DENTON: Object to form.

19 A. I heard him say he imaged everything.

20 Q. (By Mr. Havian) Okay.

21 A. And then he referenced poll pads.

22 Q. If it turns out that you misheard and he
23 didn't say he -- that they imaged the poll pad or
24 didn't mean that, would that affect your view about
25 whether he was a suspect person providing this

1 information?

2 A. Just the whole conversation sounded suspect
3 to me. I would want -- I would want somebody
4 technically competent to go assess before I jump to
5 any conclusions.

6 Q. Okay.

7 A. I have seen too many people brag that they
8 could do something in this job only to find out they
9 weren't even close to doing what they said they were
10 doing.

11 Q. Okay.

12 Getting back to the specifics of the
13 conversation, aside from the comment about imaging
14 the poll pad, was there anything else that he said in
15 the conversation that struck you as not plausible?

16 A. I would have to listen to it a few times.
17 But the fact that he even said that he was -- that
18 somebody in the department gave them access to image
19 the equipment, first would be who would have done
20 that? I would ask to go back to Coffee County and
21 talk to the elections people there and say "Did you
22 actually do this" or "Is this guy" -- so until you
23 can tell me that you have got corroborating evidence
24 from somebody else there, I would hold this whole
25 conversation in suspect.

1 Q. Yes. And I take it from your demeanor it's
2 fair to say this is such an absurdly grotesque
3 invasion of security that it's hard for you to
4 imagine it actually happened; is that fair?

5 A. Yes.

6 MR. DENTON: Object to the form.

7 Q. (By Mr. Havian) During Mr. Sterling's
8 deposition, he testified that events in Coffee County
9 were investigated in connection with the Presidential
10 election of 2020.

11 Are you aware of any such investigation?

12 A. No.

13 Q. You are not aware of any investigation of
14 events during the Presidential election of 2020 that
15 occurred in Coffee County at all; is that right?

16 MR. DENTON: Object to form.

17 A. Correct. I am not aware.

18 Q. (By Mr. Havian) So I don't want to beat a
19 dead horse. To the extent that Mr. Sterling
20 testified that there was an investigation, you are
21 just not familiar with what he's alluding, referring
22 to; is that right?

23 A. Correct. If there was an investigation
24 with a issue, it most likely would have come to me.
25 But if it was an investigation where it was found

1 that there was no issue, then he probably wouldn't
2 have told me anything about it.

3 Q. Okay. So is it correct, then, that you
4 would not be brought into the loop simply because
5 there was an investigation of an election security
6 issue? You would only be brought into the loop if it
7 was determined to be above a certain level of
8 seriousness?

9 MR. DENTON: Object to form.

10 A. I can only say from what my experience, I
11 was not brought in. There was nothing that they
12 identified that they needed the CIO of the Secretary
13 of State to get involved with. I have been involved
14 with other things, such as the Fulton County laptop.

15 Q. (By Mr. Havian) Understood. So can you
16 describe for us the threshold of the seriousness of
17 an issue before it is brought to your attention?

18 MR. DENTON: Object to form.

19 A. If something is identified as a security
20 issue that has been verified, that they need somebody
21 from the IT Department of the Secretary of State to
22 investigate, yes, I would get pulled in. If there
23 was a county issue that the counties are managing,
24 often it's left at the county level. So this one was
25 not brought to me.

1 Q. (By Mr. Havian) Okay.

2 Again, focusing on Coffee County, do you
3 recall ever hearing anything about a password being
4 shared improperly in Coffee County, a password to the
5 EMS system?

6 A. I have heard no security questions that
7 came out of Coffee County about any topic.

8 Q. Were you aware that in Coffee County, as in
9 other counties, they did a machine recount following
10 the 2020 Presidential election?

11 A. Not particularly. I think there was
12 recounts in numerous counties, and I didn't -- I
13 don't get involved with the actual voter tabulation
14 process. I focus on the systems at the state level.

15 Q. So were you aware that in Coffee County,
16 the machinery count produced a discrepancy?

17 A. Okay. I'll restate. I know nothing
18 specific about Coffee County election-wise.

19 Q. Do you recall hearing about machine recount
20 discrepancies in any counties in Georgia in
21 connection with the 2020 Presidential election?

22 A. I recall hearing accusations. I never
23 heard of any actual proven issues.

24 Q. Okay. Do you recall anything more specific
25 about the accusations you heard?

1 A. No. It was quite a while back.

2 Q. I'm going to ask you to take a look at the
3 next exhibit, which will be Exhibit 13.

4 MR. HAVIAN: Joe, can you upload the
5 November 2020 memo, please?

6 (Plaintiffs' Exhibit 13, Official Election
7 Bulletin, dated November 17, 2020, from Chris
8 Harvey, Elections Division Director, to County
9 Election Officials and County Registrars, RE:
10 Open Records Requests - Security Information
11 Exempt, marked for identification.)

12 Q. (By Mr. Havian) And while we are doing
13 that, do you recall any information about Coffee
14 County declining to certify their results after a
15 machine recount?

16 A. As I stated before, I have no knowledge of
17 anything that was tied to Coffee County. Prior to
18 this conversation, I can't tell you I have ever even
19 heard anything about Coffee County as the county.

20 Q. Okay. Can you please pull up Exhibit 13?

21 A. Election Bulletin, November 17?

22 Q. Correct. And you may need to enlarge it on
23 your screen in order to read it.

24 A. Yes.

25 Q. Let me know when you've got it to the point

1 where it's legible. Sorry about that.

2 A. I can see it.

3 Q. Okay. So first of all, take a look at this
4 memo, which is from Chris Harvey, Elections Division
5 Director, to County Election Officials and County
6 Registrars, dated November 17th, 2020. And I would
7 like to ask you if you recognize this memo.

8 A. No.

9 Q. You don't believe you have seen it before?

10 A. I know I haven't seen it before.

11 Q. I would like to ask you a few questions to
12 see if some of these things are familiar to you, even
13 though I appreciate you haven't read the memo before.

14 First of all, do you know Mr. Harvey?

15 A. Yes.

16 Q. And who is he?

17 A. He was the Director for Elections.

18 Q. And do you know generally what his
19 responsibilities were as Director of Elections?

20 A. So he was responsible for running the
21 state-level responsibilities for running elections.
22 So that means managing the voter registration system,
23 collecting anything that was tied to the voter
24 registration system. They managed the election
25 ballot count collection process.

1 Counties actually are responsible, by law,
2 to actually run the elections and actually run the
3 machines. So he did not manage that. But he did act
4 as an adviser to the counties on the election law.

5 Q. Okay. So I would like to have you look at
6 this memo and I would like to read a couple of short
7 parts of it to you.

8 First, I want to start in the second
9 paragraph --

10 A. Yes.

11 Q. -- where Mr. Harvey says "Several counties
12 have also received Open Records Requests for the
13 information contained in the log files of the KNOWiNK
14 poll books."

15 Do you see that?

16 A. Yes.

17 Q. And then he's -- going down a couple of
18 paragraphs, in the second to last paragraph, he says
19 "Under the Open Records Act, providing copies of
20 software, software updates, or thumb drives
21 containing software or software updates is not
22 subject to open records requests."

23 Do you see that?

24 A. Yes.

25 Q. And then later at the bottom of the first

1 page, there's the last couple lines -- well, actually
2 it's a fairly long sentence there. But basically, he
3 says he cannot give out software or databases except
4 upon the order of a court of competent jurisdiction.

5 Do you see that?

6 A. Yep.

7 Q. Do you know why -- do you know of any
8 reason why Mr. Harvey sent out a memo warning people
9 about turning over copies of software, election
10 software at this particular moment in November 2020?

11 A. Based on the first paragraph, it sounds
12 like a lot of counties were getting requests for
13 copies. So I think he -- my guess is he was
14 reiterating to make sure that everybody knew the
15 rules.

16 Q. Do you recall, in your role as Chief
17 Information Officer, that there was quite a bit of
18 discussion around this time period about people
19 trying to get ahold of copies of election software?

20 A. Yes.

21 Q. What do you recall about those discussions?

22 A. Just that we had moved to a new system.
23 There were people out that had gotten a copy of
24 similar systems of our old and tried to prove that
25 you could breach them, although nobody was ever

1 actually able to prove that. We have never found
2 anything in the old system, and I think people now
3 that they have a new system, they were just going to
4 try to redo the same exercises of trying to prove
5 that you could breach the new system.

6 Q. Can you explain what are the reasons that
7 election software is not released to the public? I
8 think you've already touched on this quite a bit in
9 your earlier testimony.

10 A. It's pretty obvious. You don't expose
11 your -- basically your system to the public because
12 they -- basically you're giving them a road map to
13 how to basically get in and access the system. So
14 the best defense of any system is keeping everything
15 secret about that system.

16 Q. Has your department ever issued
17 recommendations to physically secure software against
18 unauthorized use or copying?

19 A. My department, you mean the IT Department?

20 Q. Yes.

21 A. We have had conversations with both our
22 counsel and the Elections Department in general of
23 how to communicate different types of security
24 measures to the county. Often Chris Harvey would
25 come to us and say "Hey, I have got to talk to the

1 counties about this issue, it could be a security
2 issue' or something like that and ask how to phrase
3 it to make sure that it complies with, you know, best
4 practices. Things like that.

5 Is that what you are asking?

6 Q. That's among them, yes. And do you recall
7 any such conversations shortly after the 2020
8 election?

9 A. I don't recall anything. It doesn't mean
10 it didn't happen because Chris sent messages out to
11 the counties all the time, and he would come consult
12 with me on occasion to help word his messages.

13 So he may have. I don't keep track or
14 records of them. It was just -- they were
15 conversations.

16 Q. Did they have any particular urgency, those
17 conversations, in the aftermath of the 2020 election?

18 A. I don't have any record of that.

19 Q. Are there protocols in place at the
20 Secretary of State if there is a suspicion that
21 there's been an unauthorized access of election
22 software?

23 A. We have an Incident Response Plan that we
24 walk through, basically if something comes up that we
25 will walk through to collect information to determine

1 whether we had an event.

2 Q. Can you describe briefly for us the steps
3 of that Incident Response Plan?

4 A. Essentially, first, is to go collect -- you
5 know, collect information initially of what the event
6 was. So, for example, the Fulton County laptop
7 issue, it was -- it was an event. It then turned out
8 it was not an incident. They are different.

9 So the first thing to do is you collect
10 information from that source. Often we will go
11 directly to, like, Investigations to help us do the
12 research. We will notify the department head, like,
13 that would have been Chris Harvey. We'd have
14 notified Gabe Sterling of it and Ryan Germany, so the
15 key leadership structure, that this is going on.

16 And then we would start our investigation.
17 In some situations when it seems that we need more
18 high-end forensics, we will bring in an outside
19 source. So we have a company called Fortalice that
20 helps us do forensics work if it's specifically that
21 type of work. And we will go through and collect
22 that.

23 Oftentimes we will reach out to -- we have
24 contacts at both Homeland Security and FBI and GBI,
25 for Georgia Bureau of Investigation, and we will work

1 with -- so we have direct contacts to them. They are
2 used to us contacting them on events like this and
3 they go through their process for helping us research
4 it to determine whether this is -- this is really
5 something, an issue or just more of a scare.

6 Q. You mentioned that there is a distinction
7 between an incident and an event. What's that
8 distinction?

9 A. Well, when somebody first declares "Oh,
10 this is a problem," we don't call it an incident.
11 It's an event. So we have to basically find out is
12 it real? Is it something -- because once it gets to
13 an incident, then you've got to figure out and start
14 establishing a recovery plan and damage control. But
15 we don't jump into all of those things until we
16 actually can prove that this was real.

17 So it's -- we have lots of events.
18 Incidents rarely, if ever, happen.

19 Q. So is it fair to say, then, that something
20 being elevated from an event to an incident is a
21 matter of how much proof there is that you find when
22 you look at it initially?

23 A. That's essentially how you transition.
24 Someone could say that, that they hacked the system.
25 Okay. So we have this -- we all go do an

1 investigation of that. We may find, well, they
2 really didn't hack the system. What they did was
3 this, this and this.

4 So our, you know, remediation may be
5 anything from it's a hoax, to oh, it's something that
6 looks, like, bad, but it really isn't, to oh, we have
7 got damage control we have got to do. That's an
8 incident. I have got to -- probably end up having to
9 report it.

10 The Secretary of State's going to get
11 involved. We may have to report to the press.
12 There's a number of things that we will probably have
13 to do. But events, those are just day-to-day things
14 that you work.

15 Q. So when something goes from an event to an
16 incident, do you become involved at that point if
17 it's a security issue?

18 A. It differs. I get pulled in a lot on
19 events. The Fulton County one I got pulled into.
20 The Coffee County one I didn't. Coffee County hasn't
21 turned into an incident yet.

22 Q. Okay. And who would be the person in the
23 Secretary of State's organization most likely to hear
24 about some sort of improper access, even if it didn't
25 rise to the level of an incident but was only an

1 event?

2 A. It depends on where it happens. If it
3 happens in the counties, Chris Harvey might have
4 heard of it. But he worked with the county to find
5 out what happened.

6 I mean, we will get messages from counties
7 saying that e-mails have been compromised and they
8 don't know whether or not they have hacked into the
9 system. And so the county level will go through and
10 send Chris Harvey a message saying this is what they
11 are doing to evaluate it. And then when they have
12 resolved what happened, they will let him know. And
13 if it doesn't deem that it was impacting our system,
14 he wouldn't let me know.

15 Q. All right. So -- and again, just so I
16 understand this correctly, if something happens at
17 the county level but it's an incident that is
18 deemed -- or rises to the level of an incident and
19 involves election security --

20 A. I will hear about it.

21 Q. What's that?

22 A. I will hear about it.

23 Q. You will hear about it. So in other words,
24 it can't just -- something that I've just described
25 can't be resolved properly at the county level and

1 the state has to get involved; is that fair?

2 MR. DENTON: Object to the form.

3 A. Traditionally, in the past, I have heard
4 about it if it -- if it truly has happened.

5 Q. (By Mr. Havian) Okay. And when you say --
6 I think you mentioned that you were describing the
7 process that Investigations gets involved. Can
8 you -- is there a specific department that you were
9 referring to there?

10 A. So we have an Investigation Department.
11 Frances -- Ms. Frances was heading that department.
12 So she -- she might get pulled in. If it is
13 something that needs more technical investigation,
14 that's why we use Fortalice to do our forensics work
15 there.

16 It all depends on the type of
17 investigation. It may be just something that
18 department heads can work through. If it's a county
19 level, the county is going to have to go through.
20 They're the ones that basically manage and own their
21 process.

22 Q. Okay.

23 Let's go back to Exhibit 13, the Harvey
24 memo for a moment.

25 A. Yes.

1 Q. Again, that second paragraph that I read
2 out loud referred to log files in the poll books.

3 Do you see that?

4 A. Yes.

5 Q. Can those log files be copied?

6 A. I have never heard of anybody being able to
7 do that. But, I mean, we would have to talk to
8 KNOWiNK to know whether or not they have a process
9 for getting log files off of those -- those iPads.

10 Q. Well, Mr. Harvey's memo suggested they can
11 be copied, doesn't it? Because the next sentence
12 says "The information stored in the log files may not
13 be produced, as it contains information that is
14 protected under the Georgia Trade Secrets Act of 1990
15 and the Open Records Act."

16 Do you see that?

17 MR. DENTON: Object to the form.

18 A. That doesn't mean that he knows that you
19 can do it. He's just stating if somebody has asked
20 for them, then you are not to try getting them off,
21 if they even exist on there. I mean, from this
22 conversation, I don't even know if KNOWiNK has log
23 files. But somebody has to ask for them.

24 Q. (By Mr. Havian) You don't think it reflects
25 negatively on Mr. Harvey's credibility, do you, that

1 he believes that it's possible to copy that
2 information from the poll books, do you?

3 MR. DENTON: Object to form.

4 A. Chris Harvey was not a technical person.

5 Q. (By Mr. Havian) Right. But you believe --

6 A. So he wouldn't know whether you could or
7 could not. From the conversation in Paragraph 1, it
8 looks like somebody is making an Open Records Request
9 for things like log files. So its message is
10 basically saying whether it's there or not, you are
11 not allowed to get it out. I doubt he would know
12 whether or not a log file existed on a poll pad. In
13 fact, I would be surprised if he even understood what
14 a log file was.

15 Q. I'm sorry if I interrupted your answer a
16 little bit there, Mr. Beaver. There is a little bit
17 of a lag here. So I just want you to -- but I
18 appreciate your answer.

19 My question, though, is you don't believe
20 that Mr. Harvey suggesting that this was a
21 possibility reflects negatively on his credibility,
22 do you?

23 A. No.

24 Q. Okay. And you know Mr. Harvey, you have
25 worked with him, correct?

1 A. Correct.

2 Q. Do you respect his ability?

3 A. Yes.

4 Q. Do you think he's competent in his job?

5 A. Very.

6 Q. When you earlier referred to Frances,
7 someone named Ms. Frances, excuse me, I may have
8 misheard you. Were you referring to Frances Watson?

9 A. Yes.

10 Q. Does she still work for the Secretary of
11 State's Office?

12 A. No.

13 Q. Do you know when she left?

14 A. I think it was the last six months.

15 Q. I have to ask you another name.

16 Have you ever heard the name Misty Martin
17 or Misty Hampton? Is that name familiar?

18 A. No. No.

19 Q. You were not aware that she was terminated
20 from her position in Coffee County, right?

21 A. That would be correct since I don't know
22 anything about Coffee County.

23 Q. And just to be clear on your testimony,
24 Mr. Beaver, you are not taking -- it's not your
25 understanding that poll pads cannot have anything

1 imaged or exported, it's just simply that you don't
2 know whether that's true or not; is that fair?

3 A. That's fair.

4 MR. DENTON: Object to form.

5 MR. HAVIAN: Can we go off the record for a
6 bit? I just want to gather my final thoughts
7 and then I will wrap up. So can we just take a
8 five-minute break?

9 THE VIDEOGRAPHER: The time is 12:59. We
10 are off the record.

11 (WHEREUPON, a recess was taken.).

12 THE VIDEOGRAPHER: The time is 1:04. We
13 are back on the record.

14 Q. (By Mr. Havian) Mr. Beaver, just one last
15 area.

16 If someone were to obtain an image of the
17 election software, can you give some examples of some
18 of the bad things that someone who had malintent
19 could do with that?

20 MR. DENTON: Object to form.

21 A. It will be speculation only. But if
22 somebody has a copy of software, you could
23 essentially go through and get a better understanding
24 of how it works, and basically practice defeating its
25 security. Because no software is someone can walk up

1 to it without any prior knowledge to it and just
2 defeat it.

3 So you would have to have -- if you want to
4 defeat a piece of software, you are going to have to
5 have a copy of it. It's kind of like an operating
6 system. To defeat the security in an operating
7 system, you will have to practice defeating it and
8 coming at -- and using the words I used before,
9 "different vectors" to see which ones could actually
10 do it.

11 So that if somebody had a copy, then they
12 would give them the ability to go find the different
13 vectors to come at it to defeat it.

14 Q. (By Mr. Havian) And if someone were able to
15 defeat the software security, can you explain what
16 the -- kind of a worst case scenario would be of
17 someone gaining access?

18 A. So -- and could you tell me which piece of
19 equipment you are talking about?

20 Q. Election machinery.

21 A. Okay. And that's a broad spectrum.

22 MR. DENTON: Object to form.

23 A. So election machinery includes lots of
24 pieces and parts. Are you talking about the ballot
25 marking device, the scanner --

1 Q. (By Mr. Havian) How about the EMS server?

2 A. The EMS server. So that is -- you are
3 talking about the ballot building system?

4 Q. Yes.

5 A. So that's the Dominion software?

6 Q. Yes.

7 A. Okay. So the Dominion software, which sits
8 in an air-gapped environment, even if you had the
9 software, the vectors to attack it are very small.
10 So that would have limited them to some very, very
11 tight criteria of how you could attack it,
12 considering it's not connected to any Intranet
13 network.

14 Basically you have got a USB port on a
15 machine, and so you would have to deal with just a
16 very small amount of vectors to get to it. And we
17 have put layers and layers of security on how data is
18 transferred through those USB ports, even.

19 So having a copy of that, you would get an
20 idea what to go after, but the vectors of attack are
21 so small, it would be -- even with the software, it
22 would be really hard to come up with a scenario that
23 could get there. It would be near impossible.

24 That was the whole purpose of putting that
25 software in an air-gapped environment is that we

1 limited the access to basically a USB port and what
2 we call sneaker net. And the devices that are
3 allowed to go into that machine are not only
4 formatted, double scanned and assessed as to what's
5 in there with keys, that would be really difficult to
6 penetrate. So you would have to know all the other
7 parts of the security system, even once you had the
8 Dominion software, to get on to it.

9 Q. So is there any way to get data connection
10 into the EMS software through internal networks?

11 A. No. That's the whole idea. That's the
12 whole idea of the environment. It is completely
13 blocked off. It doesn't even share anything but
14 electricity in the building. It is an island.

15 Q. And how about the tabulation and reporting
16 machinery?

17 A. So the tabulation, you are talking election
18 night reporting?

19 Q. Yes.

20 A. So the Scytl system. So that is run by
21 Scytl. It runs in the cloud. The counties send data
22 to that that gives basically the counts to the press
23 and what people report, you know, winners.

24 But the actual certification process does
25 not come through that. It comes directly from the

1 counties in a separate path, and that's what is
2 certified. So if somebody was to hack, let's say,
3 Scytl and change the tabulation numbers, when it came
4 down to certifying, it would have -- it would be
5 revealed that it was hacked.

6 Q. So I'm really trying to focus in on the
7 county level. The counties do tabulation, the
8 counties have an EMS system as well, right?

9 A. The counties have ballot marking devices
10 that they collect their data from. Is that what
11 you're ask -- well, they don't collect the data from
12 the ballot marking devices. They collect the data
13 from the scanners and the scanners -- and get --

14 Q. And they have EMS servers?

15 A. -- compiled. Yes, but they get compiled.
16 And so they have got a paper receipt that says "This
17 is what just came off this ballot." And those get
18 posted on a window or some public place for people in
19 the public to see, and then we electronically pull
20 them together.

21 So the comparison of those numbers is easy
22 to do. So if somebody got in and decided,
23 electronically, to hack the process, that would also
24 be easily determined that it was compromised by just
25 doing a simple comparison between the posted numbers,

1 that were a hard copy, and the electronic numbers.
2 So at the county level they have got double
3 protection.

4 Q. I understand there are protections. I'm
5 just trying to find out what would happen if you
6 compromised the security of a county EMS server.

7 A. So --

8 MR. DENTON: Object to form.

9 A. You know, I would have to have somebody do
10 the forensics of what that might happen. But it
11 would -- the tabulation, the summations would
12 potentially be wrong. And they would mismatch with
13 the hard copies of what's being posted.

14 So if they were to compromise that, your
15 initial reporting might be off. But then when they
16 go and certify, it would be verified that there's a
17 problem.

18 Q. (By Mr. Havian) So if I understand you
19 correctly, you are saying that yes, the electronic
20 results would be incorrect if someone compromised the
21 EMS server. However, you could find it if you knew
22 to compare with the physical ballots. Is that your
23 testimony?

24 A. Not the physical ballot, but the ballot
25 scanning device actually generates a paper report.

1 So by looking at that tabulation you could start
2 doing comparisons. So there is checks and balances
3 to look for exactly what you are describing.

4 MR. HAVIAN: Just give me one moment.

5 All right. I don't think I have any
6 further questions. Thank you very much,
7 Mr. Beaver.

8 MR. DENTON: Mr. Beaver, I have a couple of
9 questions for you, assuming those are all of our
10 Plaintiff representatives.

11 THE WITNESS: Okay.

12 EXAMINATION

13 BY MR. DENTON:

14 Q. Okay. Will you please pull back up what
15 Mr. Havian marked as Exhibit 11. And this is the
16 Notice of Deposition and please scroll back to
17 Topic 10.

18 A. Okay. I'm there.

19 Q. Mr. Beaver, did you prepare to provide
20 testimony today in response to the topic described in
21 Topic 10?

22 A. My preparation was to read through this and
23 understand what the question was.

24 Q. Right. And from your understanding of the
25 question, it involves an actual unauthorized person

1 accessing voting data from a Georgia election of
2 images of voting equipment used in a Georgia
3 election. Is that your understanding of what that
4 topic is about?

5 A. Yes.

6 Q. And if something like that had occurred, is
7 that something that you would have known about?

8 A. Absolutely.

9 Q. And so because of that, would there have
10 been any reason for you to ask anyone else in the
11 Secretary's Office whether something like this had
12 happened for purposes of preparing for this
13 deposition?

14 A. No. I would have known already.

15 MR. DENTON: I believe those are all my
16 questions for you, Mr. Beaver. Thank you.

17 THE WITNESS: All right. Does this mean we
18 are done?

19 MR. HAVIAN: That's all, unless David has
20 any questions.

21 MR. CROSS: I do not.

22 THE VIDEOGRAPHER: This concludes the
23 videotaped deposition. The time is
24 approximately 1:14 p.m. We are off the record.

25 (WHEREUPON, the proceedings were concluded

1 at 1:14 p.m.)
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 C E R T I F I C A T E

2 STATE OF GEORGIA)

3) ss.:

4 FULTON COUNTY)

5

6 I, Robin Ferrill, Certified Court Reporter within
7 the State of Georgia, do hereby certify:

8 That MERRITT BEAVER, VOLUME II, the witness
9 whose deposition is hereinbefore set forth, was duly sworn
10 by me and that such deposition is a true record of the
11 testimony given by such witness.

12 I further certify that I am not related to any
13 of the parties to this action by blood or marriage; and
14 that I am in no way interested in the outcome of this
15 matter.

16 IN WITNESS WHEREOF, I have hereunto set my
17 hand this 25th day of March, 2022.

18 <%13637,Signature%>

19

20 ROBIN K. FERRILL, RPR

21

22

23

24

25

1 Alexander Denton, Esquire

2 adenton@robbinsfirm.com

3

4 RE: Curling, Donna v. Raffensperger, Brad

5 3/10/2022, Sanford "Merritt" Beaver

6 The above-referenced transcript is available for
7 review.

8 Within the applicable timeframe, the witness should
9 read the testimony to verify its accuracy. If there are
10 any changes, the witness should note those with the
11 reason, on the attached Errata Sheet.

12 The witness should sign the Acknowledgment of
13 Deponent and Errata and return to the deposing attorney.
14 Copies should be sent to all counsel, and to Veritext at
15 cs-midatlantic@veritext.com

16

17 Return completed errata within 30 days from
18 receipt of testimony.

19 If the witness fails to do so within the time
20 allotted, the transcript may be used as if signed.

21

22 Yours,

23 Veritext Legal Solutions

24

25

1 Curling, Donna v. Raffensperger, Brad

2 Sanford "Merritt" Beaver, (5127735)

3 E R R A T A S H E E T

4 PAGE _____ LINE _____ CHANGE _____

5 _____

6 REASON _____

7 PAGE _____ LINE _____ CHANGE _____

8 _____

9 REASON _____

10 PAGE _____ LINE _____ CHANGE _____

11 _____

12 REASON _____

13 PAGE _____ LINE _____ CHANGE _____

14 _____

15 REASON _____

16 PAGE _____ LINE _____ CHANGE _____

17 _____

18 REASON _____

19 PAGE _____ LINE _____ CHANGE _____

20 _____

21 REASON _____

22 _____

23 _____

24 Sanford "Merritt" Beaver Date

25 _____

1 Curling, Donna v. Raffensperger, Brad
2 Sanford "Merritt" Beaver (#5127735)

3 ACKNOWLEDGEMENT OF DEPONENT

4 I, Sanford "Merritt" Beaver, do hereby declare that I
5 have read the foregoing transcript, I have made any
6 corrections, additions, or changes I deemed necessary as
7 noted above to be appended hereto, and that the same is
8 a true, correct and complete transcript of the testimony
9 given by me.

10

11

12 _____
Sanford "Merritt" Beaver Date

13 *If notary is required

14

SUBSCRIBED AND SWORN TO BEFORE ME THIS

15

_____ DAY OF _____, 20____.

16

17

18

19

NOTARY PUBLIC

20

21

22

23

24

25